

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **18 DEC. 1998**

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b) —

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : (1) 42.94.52.52 Télécopie : (1) 42.93.59.30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES **17 DEC 1997**
N° D'ENREGISTREMENT NATIONAL **97 16008 -**
DÉPARTEMENT DE DÉPÔT **75**
DATE DE DÉPÔT **17 DEC. 1997**

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Patrick Richard
THOMSON multimedia
46 Quai Alphonse Le Gallo
92648 BOULOGNE

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

☒ demande initiale
☐ brevet d'invention

n° du pouvoir permanent **PG 6076** références du correspondant **PF970057** téléphone **0141865000**

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

PROCEDE D'AUTHENTIFICATION D'IMAGES NUMERIQUES ET DISPOSITIF METTANT EN OEUVRE LE PROCEDE

3 DEMANDEUR (S) n° SIREN **333773174** code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

THOMSON multimedia

Forme juridique

S.A.

Nationalité (s) **Française**

Adresse (s) complète (s)

**46 Quai Alphonse Le Gallo
92648 BOULOGNE**

Pays

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine numéro date de dépôt nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)

Patrick RICHARD

P. Richard

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRES ENREGISTREMENT DE LA DEMANDE À L'INPI

[Signature]

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Petersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

9715008

TITRE DE L'INVENTION : PROCÉDE D'AUTHENTIFICATION D'IMAGES NUMÉRIQUES ET DISPOSITIF
METTANT EN ŒUVRE LE PROCÉDE

LE(S) SOUSSIGNÉ(S) THOMSON multimedia

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

- CHEVREAU Sylvain
- MEUNIER Paul-Louis
- BOYER Robert
- STARON Alain

domiciliés à :

THOMSON multimedia
46 Quai Alphonse Le Gallo
92648 BOULOGNE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

17 Décembre 1997

Patrick Richard

P. Richard

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
12, 13	-	-	RTT	6 Mai 1998 (pas de tampon d'arrivée INPI)	14 MAI 1998 B E P

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifiées).

PROCEDE D'AUTHENTIFICATION D'IMAGES NUMERIQUES ET DISPOSITIF METTANT EN OEUVRE LE PROCEDE

5 La présente invention concerne un procédé d'authentification de données numériques et un dispositif mettant en oeuvre le procédé.

 L'invention s'applique plus particulièrement à l'authentification d'images numériques issues d'un appareil de prise de vues tel que, par exemple, une tête de caméra ou un appareil photographique.

10 Les images numériques sont des images falsifiables. Ainsi en est-il, par exemple, des images numériques constituant un reportage d'actualités ou une émission de télévision, que ces images soient diffusées en direct ou à partir d'une source de données enregistrées.

 Les personnes à qui sont transmises des images numériques se trouvent
15 donc dans une situation où l'authenticité des informations qu'elles reçoivent n'est pas garantie. Cet inconvénient est d'autant plus important que se multiplient les sources d'informations telles que, par exemple, les sources d'informations provenant de journalistes communément appelés journalistes "free-lances".

 L'invention ne présente pas cet inconvénient.

20 En effet, la présente invention concerne un procédé d'authentification d'images constituées de données numériques. Le procédé comprend :

- une étape de prélèvement, au sein des données numériques, d'au moins une première fraction des données numériques,
- une étape de hachage de la première fraction prélevée afin de générer
25 une première donnée hachée,
- une étape de déchiffrement à clé secrète K1 de la première donnée hachée de façon à constituer une signature de la première donnée hachée,
- une étape de multiplexage des données numériques et de la signature,
- une étape de démultiplexage des données numériques et de la
30 signature,
- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'au moins une deuxième fraction des données numériques, la deuxième fraction contenant des données de même type que les données contenues dans la première fraction,

- une étape de chiffrement à clé publique K2 de la signature de façon à constituer une donnée chiffrée, la clé publique K2 étant couplée à la clé secrète K1 selon le principe de la cryptographie à clé publique,

5 - une étape de hachage de la deuxième fraction de façon à constituer une deuxième donnée hachée,

- une étape de comparaison de la deuxième donnée hachée et de la donnée chiffrée permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

10 L'invention concerne également un procédé de signature d'images constituées de données numériques. Le procédé comprend :

- une étape de prélèvement, au sein des données numériques, d'au moins une première fraction des données numériques,

15 - une étape de hachage de la première fraction prélevée afin de générer une première donnée hachée,

- une étape de déchiffrement à clé secrète K1 de la première donnée hachée de façon à constituer une signature de la première donnée hachée,

- une étape de multiplexage des données numériques et de la signature de façon à constituer un signal multiplexé.

20

L'invention concerne également un procédé d'authentification d'images numériques issues d'un procédé de signature tel que celui selon l'invention mentionné ci-dessus. Le procédé comprend :

25 - une étape de démultiplexage du signal multiplexé de façon à séparer les données numériques et la signature,

- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'une deuxième fraction des données numériques, la deuxième fraction contenant des données de même type que les données contenues dans la première fraction,

30

- une étape de chiffrement à clé publique K2 de la signature de façon à constituer une donnée chiffrée, la clé publique K2 étant couplée, selon le principe de la cryptographie à clé publique, à la clé secrète K1 du procédé de signature,

- une étape de hachage de la deuxième fraction de façon à constituer une deuxième donnée hachée,

- une étape de comparaison de la deuxième donnée hachée et de la donnée chiffrée permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

5 L'invention concerne également un premier sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques. Le premier sous-ensemble comprend un appareil de prise de vues et un élément de sécurité, l'appareil de prise de vues comprenant un circuit d'interface avec l'élément de sécurité, un circuit de multiplexage et un circuit de hachage d'au
10 moins une première fraction des données numériques de façon à générer une première donnée hachée, l'élément de sécurité comprenant un circuit de déchiffrement à clé secrète K1 de la première donnée hachée de façon à générer une signature de la première donnée hachée, la signature et les données numériques étant transmises au circuit de multiplexage de façon à constituer un
15 signal multiplexé.

L'invention concerne également un second sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques. Le second sous-ensemble comprend un appareil de prise de vues et un élément de
20 sécurité, l'appareil de prise de vues comprenant un circuit d'interface avec l'élément de sécurité et un circuit de multiplexage, l'élément de sécurité comprenant un circuit de hachage d'au moins une première fraction des données numériques provenant de l'appareil de prise de vues de façon à générer une première donnée hachée et un circuit de déchiffrement à clé secrète K1 de la
25 première donnée hachée de façon à générer une signature de la première donnée hachée, la signature issue de l'élément de sécurité et les données numériques étant transmises au circuit de multiplexage de façon à constituer un signal multiplexé.

L'invention concerne encore un appareil de prise de vues permettant de
30 transformer un signal lumineux représentant au moins une image en un signal constitué de données numériques. L'appareil comprend des moyens permettant d'authentifier les données numériques.

L'invention concerne encore un sous-ensemble permettant l'authentification de données numériques issues d'un sous-ensemble permettant d'authentifier la prise de vues d'images tel que le premier ou le second sous-ensemble selon l'invention mentionné ci-dessus ou d'un appareil tel que l'appareil selon l'invention mentionné ci-dessus. Le sous-ensemble comprend un démultiplexeur permettant de séparer les données vidéo numériques et la signature, un circuit de chiffrement à clé publique K2 permettant de calculer une donnée chiffrée à partir de la signature, un circuit de hachage d'au moins une deuxième fraction des données vidéo numériques issues du démultiplexeur de façon à générer une deuxième donnée hachée, un circuit de comparaison permettant de comparer la donnée chiffrée avec la deuxième donnée hachée de façon à constituer un signal permettant de vérifier l'authenticité des données numériques.

L'invention concerne encore une unité de contrôle permettant de traiter le signal numérique issu d'une tête de caméra. L'unité de contrôle comprend un sous-ensemble permettant l'authentification de données numériques tel que celui selon l'invention mentionné ci-dessus.

L'invention concerne encore un système permettant l'authentification d'images constituées de données numériques. Le système comprend un sous-ensemble permettant d'authentifier la prise de vues d'images tel que le premier ou le second sous-ensemble selon l'invention mentionné ci-dessus ou un appareil tel que l'appareil selon l'invention mentionné ci-dessus et un sous-ensemble permettant l'authentification de données numériques tel que celui selon l'invention mentionné ci-dessus.

Un avantage de l'invention est d'authentifier les images numériques issues d'un dispositif de prise de vues. L'invention s'applique avantageusement aussi bien au cas où les images à authentifier sont des images prises en direct qu'au cas où les images à authentifier sont des images issues d'une source enregistrée.

D'autres avantages et caractéristiques de l'invention apparaîtront à la lecture d'un mode de réalisation préférentiel fait en référence aux figures ci-annexées parmi lesquelles :

- la figure 1 représente un premier dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention ;

5 - la figure 2 représente un deuxième dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention ;

- la figure 3 représente, selon l'invention, un dispositif d'authentification d'images numériques issues d'un dispositif de prise de vues tel que celui représenté en figure 1 ou en figure 2.

10 Sur toutes les figures, les mêmes repères désignent les mêmes éléments.

La figure 1 représente un premier dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation préférentiel de l'invention.

15 Le dispositif de prise de vues est constitué d'un appareil de prise de vues 1 et d'un élément de sécurité 2. L'appareil de prise de vues 1 peut être, par exemple, une tête de caméra ou un appareil photographique. Selon le mode de réalisation préférentiel de l'invention, l'élément de sécurité est un élément détachable tel que, par exemple, une carte à puce.

20 L'appareil de prise de vues 1 comprend un objectif 3, un bloc 4 de circuits de traitement du signal issu de l'objectif 3, un circuit de hachage 5, un multiplexeur 6 et un circuit 7 d'interface avec la carte à puce.

De façon connue en soi, l'objectif 3 et le bloc 4 de circuits de traitement permettent de transformer un signal lumineux L en un signal numérique VN.

25 Selon l'invention, une fraction $F1(VN)$ du signal numérique VN est prélevée, préférentiellement de façon régulière, en sortie du bloc 4. Chaque fraction $F1(VN)$ prélevée est transmise au circuit de hachage 5. Le circuit 5 peut être un circuit électronique ou un élément logiciel. A titre d'exemples non limitatifs, la fraction $F1(VN)$ du signal numérique VN peut être composée des lignes paires ou
30 impaires d'une même image ou des données relatives à la composante de luminance d'une même image. La fraction $F1(VN)$ peut également être constituée de plusieurs trames prélevées à intervalles de temps réguliers dans le cas d'une tête de caméra ou image par image dans le cas d'un appareil photo. De façon générale, la donnée $F1(VN)$ est composée de données significatives d'une image.

Le résultat $m1$ issu de la fonction de hachage du signal $F1(VN)$ est transmis au circuit d'interface 7. La donnée $m1$ comprend, par exemple, quelques dizaines de bits.

5 Le circuit d'interface 7 permet le transfert bidirectionnel de données entre l'appareil 1 et la carte à puce 2. De façon préférentielle, le circuit 7 est un circuit d'interface série bidirectionnel au standard ISO-7816.

La carte à puce contient un circuit de déchiffrement (non représenté sur la figure) ainsi qu'une clé secrète $K1$. De façon préférentielle, la clé $K1$ est stockée dans une mémoire programmable contenue dans la carte 2. Sous l'action de la clé
10 $K1$, les données $m1$ successives transmises à la carte 2 sont déchiffrées par le circuit de déchiffrement de façon à constituer une suite de données $D(m1)_{K1}$. Chaque donnée $D(m1)_{K1}$ constitue la signature de la donnée $m1$ et donc de la fraction $F1(VN)$ d'où est issue la donnée $m1$.

Par l'intermédiaire du circuit d'interface 7, les données $D(m1)_{K1}$ sont
15 transmises de la carte à puce 2 vers une première entrée du multiplexeur 6 qui reçoit, par ailleurs, le signal numérique VN sur une deuxième de ses entrées.

Le signal $S1$ issu du multiplexeur 6 est alors composé des données numériques VN et des données $D(m1)_{K1}$. De façon préférentielle, chaque donnée $D(m1)_{K1}$ est insérée dans un en-tête associé à la fraction de donnée $F1(VN)$ qui lui
20 correspond. Selon un autre mode de réalisation de l'invention, les données $D(m1)_{K1}$ sont substituées à certaines des données VN qui sont alors perdues.

La figure 2 représente un deuxième dispositif de prise de vues permettant l'authentification d'images numériques selon le mode de réalisation
25 préférentiel de l'invention.

Le dispositif de prise de vues est constitué d'un appareil de prise de vues 8 et d'un élément de sécurité 9. L'élément de sécurité est un élément détachable tel que, par exemple, une carte à puce. L'appareil 8 peut être, par exemple, une tête de caméra ou un appareil photographique. L'appareil 8 contient les mêmes
30 circuits que l'appareil 1 décrit à la figure 1 à l'exception du circuit de hachage 5.

Selon le mode de réalisation de la figure 2, la fonction de hachage est réalisée dans la carte à puce 9. Il s'ensuit que la fraction $F1(VN)$ du signal numérique VN est transmise à la carte à puce 9.

De même que mentionné ci-dessus, le hachage de la donnée $F1(VN)$ génère une donnée $m1$ qui, déchiffrée, génère une donnée $D(m1)_{K1}$. Par l'intermédiaire du circuit d'interface 7 les données successives $D(m1)_{K1}$ sont transmises de la carte à puce 9 vers le multiplexeur 6. Le signal $S1$ issu de l'appareil de prise de vues 8 est alors généré comme mentionné précédemment.

Selon le mode de réalisation préférentiel de l'invention décrit aux figures 1 et 2, l'élément de sécurité est un élément détachable. L'invention concerne cependant un autre mode de réalisation pour lequel l'élément de sécurité n'est pas détachable. Le circuit de déchiffrement à clé secrète $K1$ et le circuit de hachage 5 sont alors tous deux intégrés dans l'appareil de prise de vues lui-même.

Un dispositif de prise de vues selon l'invention, que l'élément de sécurité soit ou non détachable, peut fonctionner, toutes choses égales par ailleurs, avec des clés de déchiffrement $K1$ ayant des valeurs différentes. Une même clé $K1$ peut alors être propre à une seule personne ou à un ensemble de personnes constituant, par exemple, un groupement de journalistes. Il s'ensuit qu'un avantage supplémentaire de l'invention est de garantir la provenance des images authentifiées.

L'utilisation d'un élément de sécurité détachable et protégé, tel que, par exemple, une carte à puce, est un avantage du mode de réalisation préférentiel de l'invention. D'une part, la carte à puce assure une fonction de clé personnelle dont la clé est secrète. D'autre part, l'utilisation d'une carte à puce implique que soit mis en oeuvre un processus d'identification mutuelle entre la carte à puce et le dispositif récepteur de la carte à puce, à savoir l'appareil de prise de vues. Il s'ensuit que le niveau de sécurité relatif aux différentes étapes mises en oeuvre dans la carte à puce et le dispositif de prise de vues est un niveau de sécurité élevé.

La figure 3 représente, selon l'invention, un dispositif d'authentification d'images numériques issues d'un dispositif de prise de vues tel que celui représenté en figure 1 ou en figure 2, que l'élément de sécurité soit ou non détachable.

Le dispositif 10 d'authentification d'images numériques comprend un démultiplexeur 11, un circuit 12 de chiffrement à clé publique $K2$, un circuit 13 de

hachage et un comparateur 14. Le démultiplexeur 11 reçoit sur son entrée un signal S1 tel que celui mentionné aux figures 1 et 2. Le signal S1 provient soit d'un dispositif de prise de vues tel que celui décrit aux figures 1 et 2, soit d'une source de données enregistrées telle que, par exemple, une bande magnétique, un disque vidéo numérique ou encore une disquette.

Le démultiplexeur 11 a pour fonction de séparer les données $D(m1)_{K1}$ des données numériques VN. Les données $D(m1)_{K1}$ sont transmises au circuit 12 de chiffrement à clé publique K2.

L'opération de chiffrement à clé publique K2 d'une donnée $D(m1)_{K1}$ conduit à calculer une donnée chiffrée $C(D(m1)_{K1})_{K2}$.

Selon l'invention, des fractions $F2(VN)$ du signal numérique VN sont prélevées en sortie du démultiplexeur 11. Le prélèvement des fractions $F2(VN)$ s'effectue à l'image du prélèvement des fractions $F1(VN)$. Ainsi, chaque fraction $F2(VN)$ correspond-elle à une fraction $F1(VN)$ et les données qui sont contenues dans la fraction $F2(VN)$ qui correspond à la fraction $F1(VN)$ sont des données de même type que les données contenues dans la fraction $F1(VN)$. Par "données de même type", il faut entendre que les données qui constituent la fraction $F2(VN)$ sont des données a priori identiques aux données qui constituent la fraction $F1(VN)$ qui lui correspond : les données sont identiques si la fraction $F1(VN)$ n'a pas été falsifiée et différentes, en tout ou partie, si la fraction $F1(VN)$ a été falsifiée.

Dans tous les cas, les données contenues dans une fraction $F2(VN)$ représentent le même signal que les données contenues dans la fraction $F1(VN)$ qui lui correspond. Ainsi, par exemple, si les données contenues dans une fraction $F1(VN)$ sont constituées des lignes paires d'une image, les données contenues dans la fraction $F2(VN)$ qui correspond à la fraction $F1(VN)$ sont-elles constituées des lignes paires de la même image.

Le circuit 13 opère le hachage des données contenues dans les fractions $F2(VN)$. L'opération de hachage effectuée par le circuit 13 est identique à celle effectuée par le circuit 5. Il s'ensuit que la donnée m2 qui est associée à une fraction $F2(VN)$ correspondant à une fraction $F1(VN)$ est identique à la donnée m1 qui est associée à la fraction $F1(VN)$ si la fraction $F1(VN)$ n'a pas été falsifiée. La donnée m2 issue du circuit 13 et la donnée $C(D(m1)_{K1})_{K2}$ sont transmises au comparateur 14.

Le signal S3 issu du comparateur 14 permet alors d'indiquer si les données numériques VN sont des données authentiques ou des données falsifiées : ce sont des données pouvant être considérées comme authentiques si chaque donnée m2 est égale à la donnée $C(D(m1)_{K1})_{K2}$ qui lui correspond, ce sont des
5 données dont on sait qu'elles ont été falsifiées si au moins une donnée m2 est différente de la donnée $C(D(m1)_{K1})_{K2}$ qui lui correspond.

Selon l'invention, le dispositif 10 d'authentification d'images peut être intégré dans une unité de contrôle recevant des images filmées par une tête de caméra.

REVENDECATIONS

1. Procédé d'authentification d'images constituées de données numériques, caractérisé en ce qu'il comprend :

- 5 - une étape de prélèvement, au sein des données numériques, d'au moins une première fraction ($F1(VN)$) des données numériques (VN),
- une étape de hachage (5) de la première fraction prélevée ($F1(VN)$) afin de générer une première donnée hachée ($m1$),
- une étape de déchiffrement à clé secrète $K1$ de la première donnée
- 10 hachée ($m1$) de façon à constituer une signature ($D(m1)_{K1}$) de la première donnée hachée ($m1$),
- une étape de multiplexage des données numériques (VN) et de la signature ($D(m1)_{K1}$),
- une étape de démultiplexage (11) des données numériques (VN) et de
- 15 la signature ($D(m1)_{K1}$),
- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'au moins une deuxième fraction ($F2(VN)$) des données numériques, la deuxième fraction ($F2(VN)$) contenant des données de même type que les données contenues dans la première fraction ($F1(VN)$),
- 20 - une étape de chiffrement à clé publique $K2$ de la signature ($D(m1)_{K1}$) de façon à constituer une donnée chiffrée ($C(D(m1)_{K1})_{K2}$), la clé publique $K2$ étant couplée à la clé secrète $K1$ selon le principe de la cryptographie à clé publique,
- une étape de hachage (13) de la deuxième fraction ($F2(VN)$) de façon à constituer une deuxième donnée hachée ($m2$),
- 25 - une étape de comparaison (14) de la deuxième donnée hachée ($m2$) et de la donnée chiffrée ($C(D(m1)_{K1})_{K2}$) permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

2. Procédé de signature d'images constituées de données numériques, caractérisé en ce qu'il comprend :

- 30 - une étape de prélèvement, au sein des données numériques, d'au moins une première fraction ($F1(VN)$) des données numériques (VN),
- une étape de hachage (5) de la première fraction prélevée ($F1(VN)$) afin de générer une première donnée hachée ($m1$),

- une étape de déchiffrement à clé secrète K_1 de la première donnée hachée (m_1) de façon à constituer une signature $(D(m_1)_{K_1})$ de la première donnée hachée (m_1),

5 - une étape de multiplexage des données numériques (VN) et de la signature $(D(m_1)_{K_1})$ de façon à constituer un signal multiplexé (S1).

3. Procédé d'authentification d'images numériques issues d'un procédé de signature selon la revendication 2, caractérisé en ce qu'il comprend :

10 - une étape de démultiplexage (11) du signal multiplexé (S1) de façon à séparer les données numériques (VN) et la signature $(D(m_1)_{K_1})$,

- une étape de prélèvement, au sein des données numériques issues de l'étape de démultiplexage, d'une deuxième fraction ($F_2(VN)$) des données numériques, la deuxième fraction ($F_2(VN)$) contenant des données de même type que les données contenues dans la première fraction ($F_1(VN)$),

15 - une étape de chiffrement à clé publique K_2 de la signature $(D(m_1)_{K_1})$ de façon à constituer une donnée chiffrée ($C(D(m_1)_{K_1})_{K_2}$), la clé publique K_2 étant couplée, selon le principe de la cryptographie à clé publique, à la clé secrète K_1 du procédé de signature,

20 - une étape de hachage (13) de la deuxième fraction ($F_2(VN)$) de façon à constituer une deuxième donnée hachée (m_2),

- une étape de comparaison (14) de la deuxième donnée hachée (m_2) et de la donnée chiffrée ($C(D(m_1)_{K_1})_{K_2}$) permettant de vérifier l'authenticité des données numériques issues de l'étape de démultiplexage.

25 4. Sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques (VN), caractérisé en ce qu'il comprend un appareil (1) de prise de vues et un élément de sécurité (2), l'appareil (1) de prise de vues comprenant un circuit d'interface (7) avec l'élément de sécurité, un circuit de multiplexage (6) et un circuit de hachage (5) d'au moins une première fraction
30 ($F_1(VN)$) des données numériques de façon à générer une première donnée hachée (m_1), l'élément de sécurité (2) comprenant un circuit de déchiffrement à clé secrète K_1 de la première donnée hachée (m_1) de façon à générer une signature $(D(m_1)_{K_1})$ de la première donnée hachée (m_1), la signature $(D(m_1)_{K_1})$ et les données

numériques (VN) étant transmises au circuit de multiplexage (6) de façon à constituer un signal multiplexé (S1).

5 5. Sous-ensemble permettant d'authentifier la prise de vues d'images
constituées de données numériques (VN), caractérisé en ce qu'il comprend un
appareil (8) de prise de vues et un élément de sécurité (9), l'appareil (8) de prise de
vues comprenant un circuit d'interface (7) avec l'élément de sécurité et un circuit
de multiplexage (6), l'élément de sécurité (2) comprenant un circuit de hachage
d'au moins une première fraction ($F1(VN)$) des données numériques provenant de
10 l'appareil de prise de vues (8) de façon à générer une première donnée hachée
($m1$) et un circuit de déchiffrement à clé secrète $K1$ de la première donnée hachée
($m1$) de façon à générer une signature ($D(m1)_{K1}$) de la première donnée hachée
($m1$), la signature ($D(m1)_{K1}$) issue de l'élément de sécurité et les données
numériques (VN) étant transmises au circuit de multiplexage (6) de façon à
15 constituer un signal multiplexé (S1).

6. Sous-ensemble selon la revendication 4 ou 5, caractérisé en ce que
l'appareil (1, 8) de prise de vues est une tête de caméra.

20 7. Sous-ensemble selon la revendication 4 ou 5, caractérisé en ce que
l'appareil (1, 8) de prise de vues est un appareil photographique.

8. Sous-ensemble selon l'une quelconque des revendications 4 à 7,
caractérisé en ce que l'élément de sécurité est une carte à puce.
25

9. Appareil de prise de vues (1, 8) permettant de transformer un signal
lumineux (L) représentant au moins une image en un signal constitué de données
numériques (VN), caractérisé en ce qu'il comprend des moyens permettant
d'authentifier les données numériques (VN).

30 10. Appareil de prise de vues (1, 8) selon la revendication 9, caractérisé
en ce que les moyens comprennent un circuit d'interface (7) avec un élément de
sécurité et un multiplexeur (6).

11. Appareil de prise de vues (1, 8) selon la revendication 10, caractérisé en ce qu'il comprend un circuit de hachage (5).

5 12. Appareil de prise de vues (1, 8) selon la revendication 9, caractérisé en ce que les moyens comprennent un circuit de hachage (5), un circuit de déchiffrement à clé secrète K1 et un multiplexeur (6).

10 13. Sous-ensemble permettant l'authentification de données numériques issues d'un sous-ensemble selon l'une quelconque des revendications 4 à 8 ou d'un appareil selon la revendication 12, caractérisé en ce qu'il comprend un démultiplexeur (11) permettant de séparer les données numériques (VN) et la signature $(D(m1)_{K1})$, un circuit de chiffrement à clé publique K2 permettant de calculer une donnée chiffrée $(C(D(m1)_{K1})_{K2})$ à partir de la signature $(D(m1)_{K1})$, un circuit de hachage (13) d'au moins une deuxième fraction $(F2(VN))$ des données
15 numériques (VN) issues du démultiplexeur (11) de façon à générer une deuxième donnée hachée (m2), un circuit de comparaison (14) permettant de comparer la donnée chiffrée $(C(D(m1)_{K1})_{K2})$ avec la deuxième donnée hachée (m2) de façon à constituer un signal (S3) permettant de vérifier l'authenticité des données numériques.

20

14. Unité de contrôle permettant de traiter le signal numérique issu d'une tête de caméra, caractérisée en ce qu'elle comprend un sous-ensemble selon la revendication 13.

25 15. Système permettant l'authentification d'images constituées de données numériques, caractérisé en ce qu'il comprend un sous-ensemble selon l'une quelconque des revendications 4 à 8 ou un appareil selon la revendication 12 et un sous-ensemble selon la revendication 13.

numériques (VN) étant transmises au circuit de multiplexage (6) de façon à constituer un signal multiplexé (S1).

5. Sous-ensemble permettant d'authentifier la prise de vues d'images constituées de données numériques (VN), caractérisé en ce qu'il comprend un appareil (8) de prise de vues et un élément de sécurité (9), l'appareil (8) de prise de vues comprenant un circuit d'interface (7) avec l'élément de sécurité et un circuit de multiplexage (6), l'élément de sécurité (2) comprenant un circuit de hachage d'au moins une première fraction (F1(VN)) des données numériques provenant de l'appareil de prise de vues (8) de façon à générer une première donnée hachée (m1) et un circuit de déchiffrement à clé secrète K1 de la première donnée hachée (m1) de façon à générer une signature (D(m1)_{K1}) de la première donnée hachée (m1), la signature (D(m1)_{K1}) issue de l'élément de sécurité et les données numériques (VN) étant transmises au circuit de multiplexage (6) de façon à constituer un signal multiplexé (S1).

6. Sous-ensemble selon la revendication 4 ou 5, caractérisé en ce que l'appareil (1, 8) de prise de vues est une tête de caméra.

7. Sous-ensemble selon la revendication 4 ou 5, caractérisé en ce que l'appareil (1, 8) de prise de vues est un appareil photographique.

8. Sous-ensemble selon l'une quelconque des revendications 4 à 7, caractérisé en ce que l'élément de sécurité est une carte à puce.

9. Appareil de prise de vues (1, 8) permettant de transformer un signal lumineux (L) représentant au moins une image en un signal constitué de données numériques (VN), caractérisé en ce qu'il comprend des moyens permettant d'authentifier les données numériques (VN), les moyens permettant d'authentifier les données numériques comprenant un circuit d'interface (7) avec un élément de sécurité et un multiplexeur (6).

10. Appareil de prise de vues (1, 8) selon la revendication 9, caractérisé en ce qu'il comprend un circuit de hachage (5).

5 11. Appareil de prise de vues (1, 8) permettant de transformer un signal lumineux (L) représentant au moins une image en un signal constitué de données numériques (VN), caractérisé en ce qu'il comprend des moyens permettant d'authentifier les données numériques (VN), les moyens permettant d'authentifier les données numériques (VN) comprenant un circuit de hachage (5), un circuit de déchiffrement à clé secrète K1 et un
10 multiplexeur (6).

12. Sous-ensemble permettant l'authentification de données numériques issues d'un sous-ensemble selon l'une quelconque des revendications 4 à 8 ou d'un appareil selon la revendication 11, caractérisé
15 en ce qu'il comprend un démultiplexeur (11) permettant de séparer les données numériques (VN) et la signature $(D(m1)_{K1})$, un circuit de chiffrement à clé publique K2 permettant de calculer une donnée chiffrée $(C(D(m1)_{K1})_{K2})$ à partir de la signature $(D(m1)_{K1})$, un circuit de hachage (13) d'au moins une deuxième fraction $(F2(VN))$ des données numériques (VN) issues du
20 démultiplexeur (11) de façon à générer une deuxième donnée hachée (m2), un circuit de comparaison (14) permettant de comparer la donnée chiffrée $(C(D(m1)_{K1})_{K2})$ avec la deuxième donnée hachée (m2) de façon à constituer un signal (S3) permettant de vérifier l'authenticité des données numériques.

25 13. Unité de contrôle permettant de traiter le signal numérique issu d'une tête de caméra, caractérisée en ce qu'elle comprend un sous-ensemble selon la revendication 12.

30 14. Système permettant l'authentification d'images constituées de données numériques, caractérisé en ce qu'il comprend un sous-ensemble selon l'une quelconque des revendications 4 à 8 ou un appareil selon la revendication 11 et un sous-ensemble selon la revendication 12.

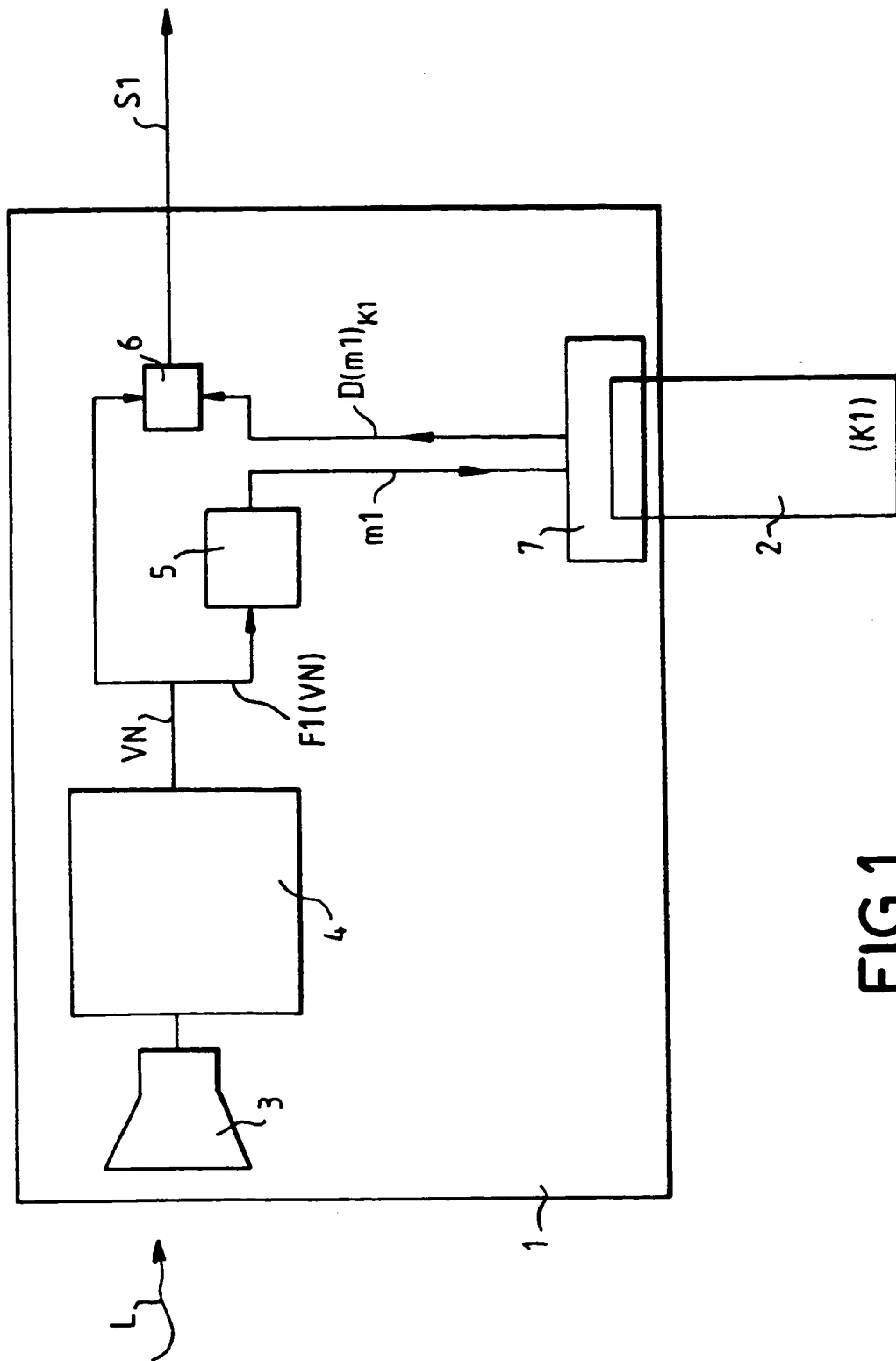


FIG.1

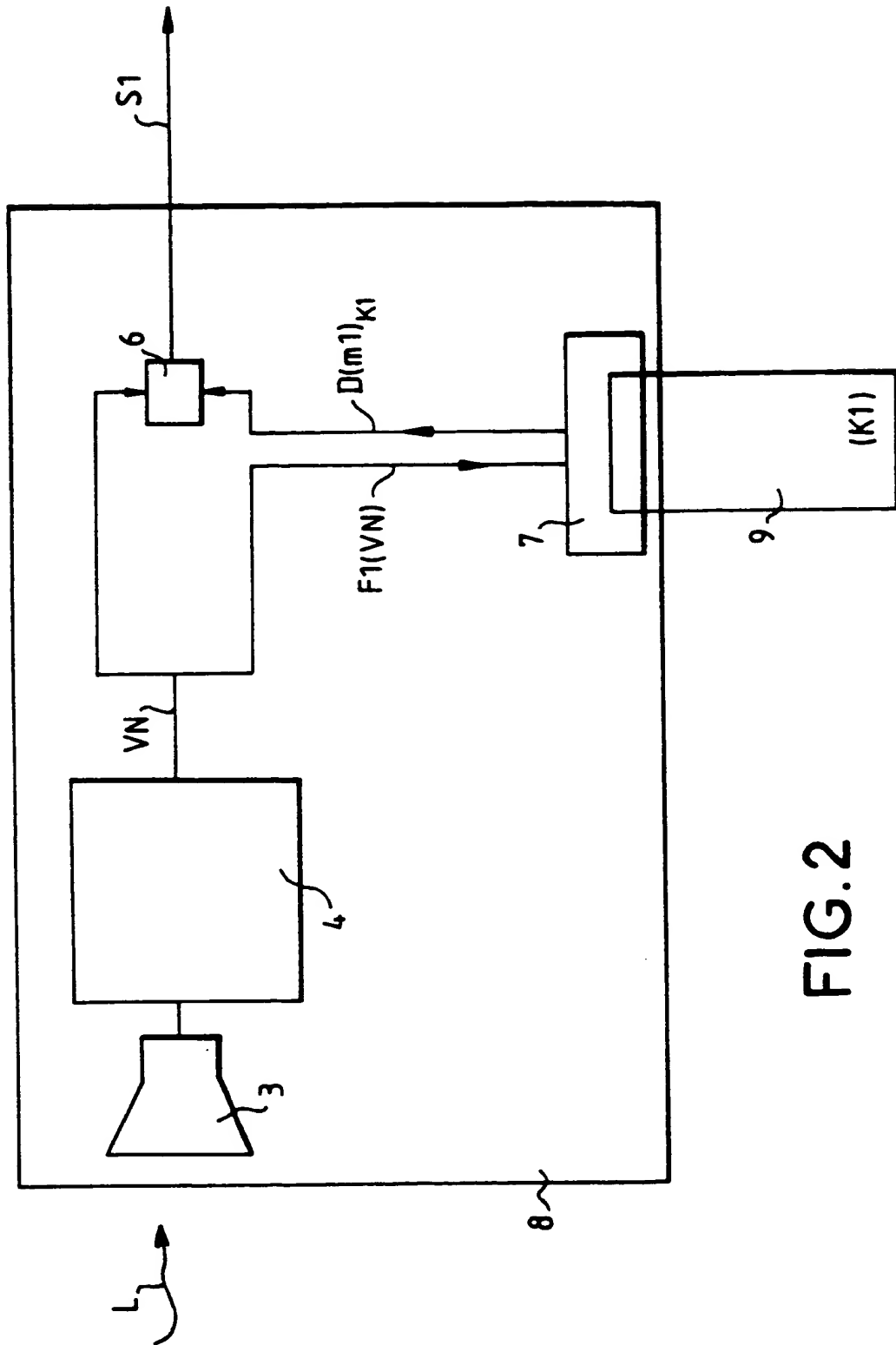


FIG.2

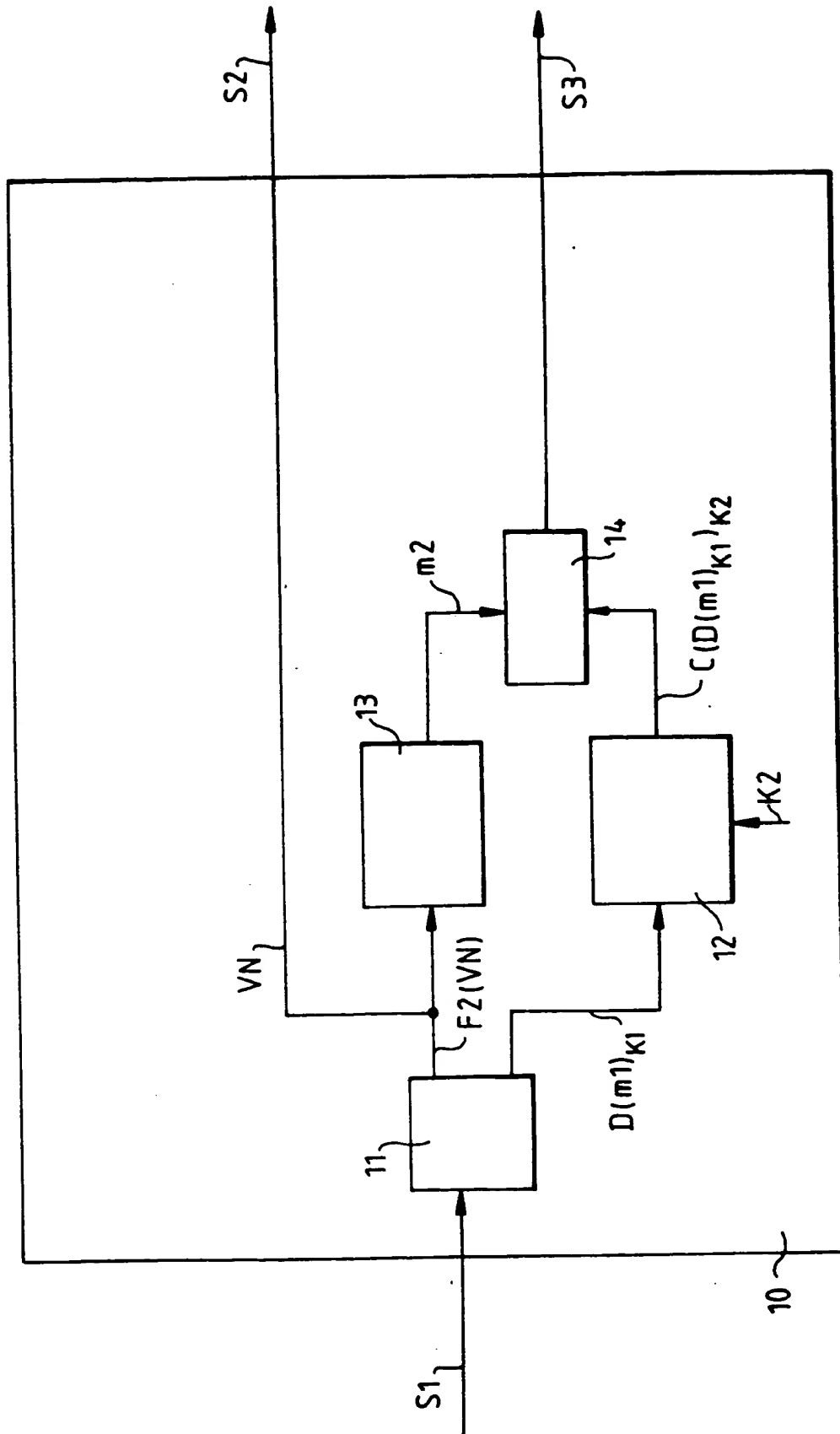


FIG. 3

THIS PAGE BLANK (USPTO)